**EKERUCHE CHINWE**

**I5/ENG02/020**

**CRYPTOGRAPHY**

**COE 522**

**AUTOKEY CIPHER**

Auto Key is a free, open-source scripting application for Linux. Hotkeys and trigger phrases may also be configured to run scripts which can use the full power of Python 3 to perform actions and to emit window, keyboard, and mouse events using the provided Auto Key API. An auto key cipher (also known as the autoclave cipher) is a cipher that incorporates the message (the plaintext) into the key. The key is generated from the message in some automated fashion, sometimes by selecting certain letters from the text or, more commonly, by adding a short primer key to the front of the message.

There are two forms of auto key cipher: key-auto key and text-auto key ciphers. A key-auto key cipher uses previous members of the key stream to determine the next element in the key stream. A text-auto key uses the previous message text to determine the next element in the key stream.



An example of a tabular recta for use with an auto key cipher

This cipher was invented in 1586 by [Blaise de Vigenère](https://en.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re) with a reciprocal table of ten alphabets. Vigenère's version used an agreed-upon letter of the alphabet as a primer, making the key by writing down that letter and then the rest of the message. More popular auto keys use a [tabula recta](https://en.wikipedia.org/wiki/Tabula_recta), a square with 26 copies of the alphabet, the first line starting with 'A', the next line starting with 'B' etc. Instead of a single letter, a short agreed-on keyword is used, and the key is generated by writing down the primer and then the rest of the message, as in Vigenère's version. To encrypt a plaintext, the row with the first letter of the message and the column with the first letter of the key are located. The letter in which the row and the column cross is the cipher text letter.

**Method of using auto key.**

The auto key cipher, as used by members of the [American Cryptogram Association](https://en.wikipedia.org/wiki/American_Cryptogram_Association), starts with a relatively-short keyword, the *primer*, and appends the message to it. If, for example, the keyword is "QUEENLY" and the message is "ATTACK AT DAWN", the key would be "QUEENLYATTACKATDAWN".

Plaintext: ATTACK AT DAWN...

Key: QUEENL YA TTACK AT DAWN....

Cipher text: QNXEPV YT WTWP...

The cipher text message would thus be "QNXEPVYTWTWP".

To decrypt the message, the recipient would start by writing down the agreed-on key again.

QUEENLY

The first letter of the key, Q, would then be taken, and that row would be found in a tabula recta. That column for the first letter of the cipher text would be looked across, also Q in this case, and the letter to the top would be retrieved, A. Now, that letter would be added to the end of the key:

**Enciphering and Deciphering with Auto key**

With the auto key cipher the keyword acts as a **primer**, upon which the rest of the key is built. To build the key stream, you first use the keyword, and then add on the plaintext as the rest of the key. This generates a key stream of sufficient length (longer than needed actually) that only the person enciphering the message would have. The key stream is certainly not random, since it will have all the same characteristics of the English language, but unlike when repeating the same keyword over and over, the plaintext will change the key in a manner that is more unpredictable to an eavesdropper. For a sample plaintext of accept the greater challenge and keyword of UNICORN, enciphering would look like:

 Key stream: UNICORNACCEPTTHEGREATERCH

 Plain text: acceptthegreaterchallenge

Cipher text: UPKGDKGHGIVTTMLVIYELEIEIL

Deciphering the message needs to work a little differently than normal, since the person receiving the message doesn't know the plaintext, and therefore can't generate the entire key stream from the start. Instead, they'll need to partially decipher the message using the keyword, and as plaintext is determined add on to the key stream.

 Key stream: UNICORN

Cipher text: UPKGDKGHGIVTTMLVIYELEIEIL

 Plain text: acc

So once you have a few letters, you can add them onto the key stream and decipher a few more.

 Key stream: UNICORNACC

Cipher text: UPKGDKGHGIVTTMLVIYELEIEIL

 Plain text: accepttheg

And keep going until...

Key stream: UNICORNACCEPTTHEG

Cipher text: UPKGDKGHGIVTTMLVIYELEIEIL

 Plain text: acceptthegreaterc

... you have the entire message.

 Key stream: UNICORNACCEPTTHEGREATERCH

Cipher text: UPKGDKGHGIVTTMLVIYELEIEIL

 Plain text: acceptthegreaterchallenge

**COMPUTER CRIMES**

Computer crimes also known as cybercrimes is the  the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. New technologies create new criminal opportunities but few new types of [crime](https://www.britannica.com/topic/crime-law). What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the [digital computer](https://www.britannica.com/technology/digital-computer), but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone’s privacy. All those activities existed before the “cyber” prefix became [ubiquitous](https://www.merriam-webster.com/dictionary/ubiquitous). Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities. Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer [data bases](https://www.britannica.com/technology/database) owned by governments and corporations. Below are some types of cyber crimes

1. **Hacking**

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the ‘hacking’) are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They’re usually technology buffs who have expert-level skills in one particular software program or language. Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation’s financial data, etc.

1. **Virus dissemination**

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. “Worms” unlike viruses don’t need a host to cling on to. They merely replicate until they eat up all available memory in the system.

1. **Logic bombs**

A logic bomb, also known as “slag code”, is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It’s not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. For example, the infamous “Friday the 13th” virus which attacked the host systems only on specific dates; it “exploded” (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

1. **Phishing**

This is a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You’ve probably received email containing links to legitimate appearing websites. You probably found it suspicious and didn’t click the link.

1. **Email bombing and spamming**

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim’s email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker’s control) as a DDoS attack.

**WAYS TO PTOTECT YOURSELF FROM CYBER CRIME**

1. **Keep everything up to date**

Keep your software and operating systems updated. To make it easy, turn on automatic updates when possible. Also, be sure to install software to scan your system for viruses and malware, to catch anything that might get through. Some of that protection is free, like Avast, which Consumer Reports rates highly.

1. **Use strong, unique passwords**

Consider starting with a favorite sentence and then just using the first letter of each word. Add numbers, punctuation, or symbols for complexity if you want, but length is more important. Make sure to change any default passwords set in a factory, like those that come with your Wi-Fi router or home security devices.

1. **Enable auto factor authentication**

Whenever you have the option, enable multifactor authentication, particularly for crucial log-ins like bank and credit card accounts. You could also consider getting a physical digital key that can connect with your computer or smartphone as an even more advanced level of protection.

1. **Encrypt and back up your most important**

Data For data that’s crucial, like medical information, or irreplaceable, like family photos, it’s important to keep copies. These backups should ideally be duplicated as well, with one stored locally on an external hard drive only periodically connected to your primary computer, and one remote, such as in a [cloud storage](https://support.apple.com/en-us/HT202303) system.

1. **Be careful using public wifi**

When using public Wi-Fi, anyone nearby who is connected to the same network can listen in on what your computer is sending and receiving across the internet. In general be Cautious, Proactive and Informed.